Listing of Claims

This listing of claims 1-2 will replace all prior versions, and listing of claims in the application.

1. (Currently Amended) A method of detecting malicious scripts using code insertion technique, comprising the step of:

checking values related to each sentence belonging to call sequences by using method call sequence detection based on rules including matching rules and relation rules,

wherein said matching rules comprise general script sentences and further include a variable string**; and**

wherein said relation rules are comprised of condition phrases and action phrases and wherein the action phrases are executed when the conditions of the condition phrase are satisfied, wherein said condition phrases are comprised of at least one condition expression for checking whether one of: (a) a rule has already been satisfied, (b) specific variable values of two rules are equal to each other, or (c) one of the specific variable values is included in the other value; and

wherein the checking step comprises the steps of:

(i) inserting a self-detection routine (malicious behavior detection routine) call sentence before and after a method call sentence of an original script; and

(ii) detecting the malicious codes during execution of the script through a self-detection routine inserted into the original script.

2. (Currently Amended) The method according to claim 1, wherein the self-detection routine call sentence **is generated by a script transformer which transforms an original script including method call sentences into a script capable of continuously performing the self-detection**

during execution through the method call sequence based on the detection rules and the self-detection routine,

wherein the self-detection routine is composed of sentences for storing parameters and return values and calling a detection engine, said sentences being inserted before and after the method call sentence when the method call sentence matches with contents described in the matching rule, and

wherein the self-detection routine includes a rule-based detection engine for executing the relation rule related to a relevant matching rule when a method corresponding to the matching rule is called and detecting the presence of malicious behavior of the method call sequence, and methods for causing the parameters and return values of the method call sentence satisfying the matching rule to be stored into a buffer usable by the detection engine.

3. (New) The method according to claim 1, further comprising selecting one rule as a higher level rule, representative of all relation rules in a set of relation rules.

4. (New) The method according to claim 1, further comprising upon satisfying the conditions of the condition phrases, generating an instance of a relation rule and thereafter checking at least one higher level rule.

5. (New) The method according to claim 4, wherein a higher level rule is a rule with a relevant rule included in its own condition expression.

6. (New) The method according to claim 1, further comprising loading matching rules and relation rules from a rule description file.

7. (New) The method according to claim 6, further comprising generating a corresponding method from each matching rule.

8. (New) The method according to claim 6, further comprising generating a corresponding method from each relation rule.

9. (New) The method according to claim 1, further comprising initializing each self-detection routine (malicious behavior detection routine) call sentence located before and after each of said method call sentences of an original script, prior to performing said continuous detection.